di Maurizio Iorio

IL REGOLAMENTO UE 2024/1689. LA PRIMA LEGGE AL MONDO SULL'USO DELL'INTELLIGENZA ARTIFICIALE

Il 1º agosto 2024 è entrato in vigore il Regolamento (UE) 1689/2024, anche detto AI Act, la prima legge al mondo volta a disciplinare il fenomeno dell'intelligenza artificiale. Con l'AI Act la UE intende salvaguardare diritti e libertà fondamentali dei cittadini; infatti, l'adozione di sistemi di IA, per certi versi potenzialmente benefica per la società, potrebbe creare seri rischi per la sicurezza, anche fisica, non solo degli utenti ma della società civile in genere. Nel presente articolo si esaminano per sommi capi le caratteristiche principali del Regolamento 1689/2024 UE.

MAURIZIO IORIO
Dalla partnership tra Marketplace e Andec prende vita questa rubrica, curata dall'Avvocato Maurizio Iorio nel suo duplice ruolo di Avvocato Professionista in Milano e di Presidente di Andec.

COS'È UN SISTEMA DI INTELLIGENZA ARTIFICIALE?

Ai fini dell'AI Act (di seguito anche il "Regolamento"), un Sistema di Intelligenza Artificiale (" Sistema IA") è «*un sistema automatizzato progettato per funzionare con livelli di autonomia variabili e che può presentare adattabilità dopo la diffusione e che, per obiettivi espliciti o impliciti, deduce dall'input che riceve come generare output quali previsioni, contenuti, raccomandazioni o decisioni che possono influenzare ambienti fisici o virtuali*».

A CHI SI APPLICA L'AI ACT?

La nuova disciplina si applicherà sia a soggetti pubblici che privati, a condizione che il Sistema di IA sia immesso sul mercato dell'Unione o che il suo impiego abbia effetti su persone situate nel territorio dell'UE. In particolare, gli obblighi stabiliti nel regolamento possono applicarsi a diversi soggetti. Si indicano qui di seguito i più importanti:

- il **Fornitore**: colui il quale sviluppa un sistema di IA o un modello di IA per finalità generali, immettendoli sul mercato con il proprio nome o marchio, a titolo oneroso o gratuito;
- il **Deployer**: colui il quale utilizza un sistema di IA sotto la propria autorità nell'ambito di un'attività professionale;
- il **Rappresentante Autorizzato**: colui il quale ha ricevuto e accettato un mandato scritto da un fornitore di un sistema di IA al fine di adempiere ed eseguire per suo conto gli obblighi e le procedure stabiliti dal Regolamento;
- l'**Importatore**: una persona fisica o giuridica ubicata o stabilita nell'Unione che immette sul mercato un sistema di IA recante il nome o il marchio di una persona fisica o giuridica stabilita in un Paese terzo;
- il **Distributore**: una persona fisica o giuridica nella catena di approvvigionamento, diversa dal fornitore o dall'importatore, che mette a disposizione un sistema di IA sul mercato dell'Unione.

CLASSI DI RISCHIO DEI SISTEMI DI INTELLIGENZA ARTIFICIALE

Il Regolamento adotta un approccio *risk-based*, nel senso di prevedere requisiti tanto più rigorosi quanto maggiori sono i rischi derivanti dai sistemi di IA per la sicurezza, la salute ed i numerosi diritti fondamentali delle persone tutelati nella Carta dei diritti fondamentali dell'UE. Le classi di rischio sono le seguenti:

- **Rischio inaccettabile**: si ha quando dagli impieghi dell'IA possono derivare conseguenze estremamente dannose: pertanto, gli stessi sono considerati vietati senza ulteriori considerazioni;
- **Rischio alto**: è la categoria di rischio su cui si concentra particolarmente il Regolamento per via della portata potenzialmente dannosa di alcuni sistemi di IA. Tra i sistemi ad alto rischio rientrerebbero, ad esempio, quelli che valutano se un individuo può ottenere un determinato posto di lavoro oppure un finanziamento per l'acquisto di una casa;
- **Rischio per la trasparenza**: è il rischio nascente da specifiche attività consistenti, ad esempio, nella generazione o manipolazione di immagini, contenuti audio e video (*deep fake*) o testi, cui sono ricollegati specifici obblighi, come l'espressa indicazione che il contenuto in questione è stato generato o manipolato attraverso un sistema di IA;
- **Rischio minimo**: è una categoria di rischio che secondo le Q&A della Commissione UE in argomento possono essere sviluppati e utilizzati nel rispetto della legislazione vigente senza ulteriori obblighi giuridici. I Fornitori di tali sistemi possono scegliere di applicare, su base volontaria, codici di condotta volontari.
- Il Regolamento prende infine in considerazione una categoria di rischio – il **rischio sistemico** – da considerarsi a sé, in quanto potenzialmente derivante non da sistemi di IA ma da **modelli di IA per finalità generali**, ovverosia modelli addestrati con grandi quantità di dati (per la complessa e più completa definizione, si rimanda all'Art. 3, punto 63 del Regolamento). Ebbene, secondo la Commissione, alcuni di questi modelli, se particolarmente efficaci o ampiamente utilizzati, potrebbero ad esempio causare incidenti gravi o essere utilizzati impropriamente per attacchi informatici di vasta portata.

Tra le classi di rischio sopra riportate, quelle a cui il Regolamento presta maggiore attenzione sono senz'altro il rischio inaccettabile, attraverso l'individuazione di pratiche vietate (ad esempio: pratiche manipolative, o che sfruttano la specifiche vulnerabilità delle persone, oppure tese ad in quadrare le persone in un sistema di social scoring), ed il rischio alto, che interessa la maggior parte del Regolamento e rispetto al quale sono **previste** norme di conformità dei sistemi di IA piuttosto complesse.

In altre parole, secondo l'approccio *risk-based* illustrato nelle Q&A della Commissione Europea, il Regolamento prevede una pluralità di obblighi prevalentemente correlati all'immissione di sistemi di IA ad alto rischio.

COSA È UN SISTEMA IA AD ALTO RISCHIO

I sistemi di IA considerati ad "alto rischio" sono quelli che hanno un significativo impatto sui diritti e sulla sicurezza degli utenti e che, ciononostante, possono essere lecitamente utilizzati a condizione che siano rispettati precisi e rigorosi requisiti e limiti.

Per esempio, la nozione di "Sistemi di IA ad alto rischio" include i sistemi in grado di valutare la meritevolezza di un individuo ai fini del suo accesso a servizi essenziali pubblici o privati, i sistemi di sorveglianza impiegati dalle forze dell'ordine, e via dicendo.

La definizione completa dei "Sistema di IA ad alto rischio" è

contenuta nell'art. 6 del Regolamento. Per una migliore comprensione, si può fare riferimento all'allegato III del Regolamento stesso, che qui non può essere riportato per evidenti ragioni editoriali ma che rappresenta ad oggi – a mio avviso – il più utile **catalogo di esempi che consentono di familiarizzare con alcuni casi d'uso concreti dell'IA (dai settori della biometria a quello dell'istruzione e dell'occupazione, dell'amministrazione della giustizia e via dicendo)**.

Con queste premessa, possiamo ora passare in rassegna i principali obblighi derivanti dall'immissione sul mercato UE di sistemi di IA ad alto rischio.

OBBLIGHI PRINCIPALI DEI FORNITORI DI SISTEMI DI IA AD ALTO RISCHIO

Uno dei principali obblighi – forse il più importante – in capo ai Fornitori di sistemi ad alto rischio consiste nel sottoporre il sistema ad una **valutazione della conformità** prima dell'immissione sul mercato UE.

Tale valutazione serve a dimostrare che il sistema di IA è conforme ai requisiti obbligatori per un'IA affidabile.

Nell'ipotesi in cui il sistema, o la sua finalità, vada incontro a modifiche sostanziali la valutazione dovrà essere ripetuta.

I Fornitori dovranno dotarsi di **sistemi di gestione della qualità** (art. 17) e del rischio per garantire la conformità ai nuovi requisiti e ridurre al minimo i rischi per gli utenti e le persone interessate, anche dopo l'immissione sul mercato.

È previsto, come nella maggior parte delle normative di armonizzazione, un **obbligo di conservazione** di specifici documenti (tra tutti, vale la pena di ricordare la **dichiarazione di conformità** ai sensi dell'art. 18, par. 1, lett.e), per i 10 anni successivi all'immissione sul mercato.

Il monitoraggio del sistema di AI dovrà essere possibile attraverso il **salvataggio automatico dei *log***, da conservare per un periodo adeguato alle finalità previste dal sistema di IA (art. 19).

I fornitori che ritengono o hanno motivo di ritenere che un sistema di IA ad alto rischio da essi immesso sul mercato o messo in servizio non rispetti i requisiti del Regolamento, dovranno adottare senza indugio le **misure correttive** per rendere conforme il sistema, ritirarlo, disabilitarlo o richiamarlo, a seconda dei casi.

Naturalmente, come in tutti i casi di immissione di beni sul mercato UE, i Fornitori dovranno **collaborare con le autorità di controllo**, fornendo tutte le informazioni ed i documenti che attestino la conformità del sistema al Regolamento.

Anche i ***log*** dovranno sempre essere

accessibili alle autorità, ove queste ne facciano richiesta. Infine, il sistema di IA dovrà sempre essere accompagnato, in formato digitale o cartaceo, da **istruzioni d'uso**.

OBBLIGHI DEGLI IMPORTATORI DI SISTEMI DI IA AD ALTO RISCHIO

Come nella quasi totalità delle normative di armonizzazione dell'UE, in capo agli Importatori sono stabiliti obblighi da soddisfare prima dell'immissione del sistema di IA sul mercato UE:

Sono stabiliti innanzitutto **obblighi di verifica**. L'Importatore dovrà verificare che:

- il Fornitore del sistema di IA ad alto rischio abbia eseguito la pertinente procedura di valutazione della conformità;
- il Fornitore abbia redatto la documentazione tecnica;
- sia apposta sul sistema la marcatura CE e che sia fornita in accompagnamento la dichiarazione di conformità UE e le istruzioni d'uso;
- il Fornitore abbia nominato un rappresentante autorizzato, nell'ipotesi in cui il Fornitore stesso non abbia sede nell'UE.

L'Importatore che abbia un motivo sufficiente di ritenere che un sistema di IA ad alto rischio non sia conforme al Regolamento, o che sia falsificato o accompagnato da una documentazione falsificata, non dovrà immetterlo sul mercato fino a quando il sistema di IA non sia stato reso conforme.

Sono poi previsti specifici **obblighi di comunicazione**:

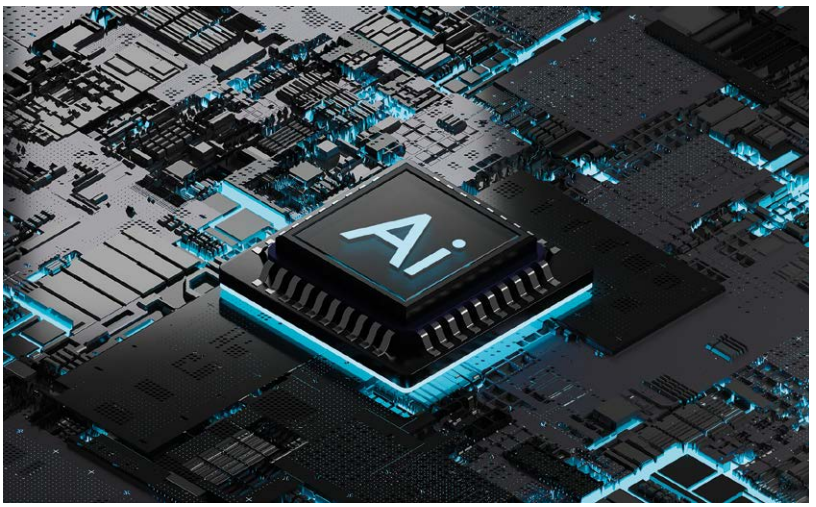
- qualora il sistema di IA ad alto rischio presenti un rischio per la salute o la sicurezza o per i diritti fondamentali delle persone, l'importatore ne informa il Fornitore del sistema, i rappresentanti autorizzati e le autorità di vigilanza del mercato.

E sono altresì stabiliti **obblighi informativi**:

- gli Importatori indicano il loro nome, la loro denominazione commerciale registrata o il loro marchio registrato e l'indirizzo al quale possono essere contattati sul sistema di IA ad alto rischio e sul suo imballaggio o in un documento di accompagnamento, ove applicabile.

I già visti **obblighi conservazione** posti in capo al Fornitore, inoltre, sono posti anche in capo all'Importatore. Infatti, ai sensi dell'art. 3, par. 25, gli importatori conservano, per un periodo di 10 anni dalla data di immissione sul mercato o di messa in servizio del sistema di IA ad alto rischio, **una copia** del certificato rilasciato dall'organismo notificato, se del caso, delle istruzioni per l'uso e della dichiarazione di conformità UE.

L'Importatore condivide col Fornitore anche l'**obbligo di collaborazione** con le autorità di controllo, in quanto, ove richiesto da quest'ultima, gli Importatori dovranno fornire tutte le informazioni e la documentazione necessaria per dimostrare la conformità di un sistema di IA ad alto rischio ai requisiti di cui alla sezione "*Requisiti per i sistemi di IA ad alto rischio*" in una lingua che possa essere compresa facilmente da tale autorità.



Per brevità, abbiamo menzionato solo alcuni tra gli obblighi e alcuni tra i soggetti più importanti coinvolti nella conformità del sistema di IA al Regolamento. Tuttavia anche altri soggetti, come il Distributore o il Deployer, sono coinvolti nella verifica dei requisiti stabiliti dal Regolamento.

SANZIONI

Le sanzioni per le violazioni dell'AI Act saranno stabilite dagli Stati Membri nell'ambito di specifiche soglie stabilite dal Regolamento:

- fino a 35 milioni di euro o il 7% del fatturato mondiale totale annuo dell'esercizio precedente (se superiore) per violazioni relative a pratiche vietate o per l'inosservanza di requisiti in materia di dati; ovvero
- fino a 15 milioni di euro o al 3% del fatturato mondiale totale annuo dell'esercizio precedente per l'inosservanza di qualsiasi altro requisito o obbligo del regolamento;
- fino a 7,5 milioni di euro o all'1,5% del fatturato mondiale totale annuo dell'esercizio precedente per la fornitura di informazioni inesatte, incomplete o fuorvianti agli organismi notificati e alle autorità nazionali competenti in risposta a una richiesta;
- per ciascuna categoria di violazione, la soglia per le PMI sarebbe l'importo più basso tra i due previsti, mentre per le altre imprese sarebbe l'importo più elevato.

TIMELINE

L'AI Act è stato pubblicato il 12 luglio 2024 nella Gazzetta Ufficiale dell'Unione europea ed è entrato in vigore il 2 agosto 2024.

L'intero Regolamento diverrà applicabile (cioè, sarà pienamente efficace) a partire dal **2 agosto 2026**, ma alcune disposizioni entreranno in vigore prima di tale data:

- i Capi I e II (Disposizioni generali e Pratiche di IA vietate) troveranno applicazione dal **2 febbraio 2025**;
- il Capo III, sezione IV (Autorità di notifica ed organismi notificati), il Capo V (Modelli di IA per finalità generali), il Capo VII (Governance) ed il Capo XII (Sanzioni) e l'art. 78 (Riservatezza) si applicano dal **2 agosto 2025**, ad eccezione dell'art. 101 (Sanzioni pecuniarie per i fornitori di modelli di IA per finalità generali);
- L'art. 6, par. 1 (Regole di classificazione per i sistemi di IA ad alto rischio) ed i corrispondenti obblighi di cui al Regolamento, a partire dal **2 agosto 2027**.